CLOUDBURST (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:23:46 UTC

CLOUDBURST aka NickelLoader is an HTTP(S) downloader.

It recognizes a set of four basic commands, all five letters long, like abcde, avdrq, gabnc and dcrqv (alternatively: eknag, eacec, hjmwk, wohnp). The most important functionality is to load a received buffer, either as a DLL via the MemoryModule implementation, or as a shellcode.

It uses AES for encryption and decryption of network traffic. It usually sends the following information back to its C&C server: computer name, product name and the list of running processes. Typically, it uses two hardcoded parameter names for its initial HTTP POST requests: gametype and type (alternatively: type and code).

The CLOUDBURST payload is disguised as mscoree.dll and is side-loaded via a legitimate Windows binary PresentationHost.exe with the argument -embeddingObject. It comes either as a trojanized plugin project for Notepad++ (usually FingerText by erinata), or as a standalone DLL loaded by a dropper, which is a trojanized plugin project as well (usually NppyPlugin by Jari Pennanen).

The CLOUDBURST malware was used in Operation DreamJob attacks against an aerospace company and a network running Microsoft Intune software in Q2-Q3 2022.

▶ [TLP:WHITE] win_cloudburst_auto (20251219 | Detects win.cloudburst.)
